Overhauling Intelligence

Mike McConnell

INTELLIGENT REFORM

Before World War II, the United States' defense, intelligence, and foreign policy apparatus were fragmented, as befitted a country with a limited role on the world stage. With U.S. entry into the war, interagency collaboration developed out of crisis-driven necessity. Wartime arrangements, although successful, were ad hoc. And after the war, President Harry Truman and Congress realized that the United States could not meet its new responsibilities without a national security structure that rationalized decision-making and integrated the intelligence and military establishments. It was against this background that on July 26, 1947—60 years ago this summer—Truman signed the National Security Act, a seminal piece of legislation for the U.S. intelligence community that laid the foundation for a robust peacetime intelligence infrastructure.

With the proper tools and public support and the help of allies, the United States built the world's premier intelligence establishment. It put spy planes in the sky, satellites into space, and listening posts in strategic locations around the world. It also invested in its people, developing a professional cadre of analysts, case officers, linguists, technicians, and program managers and trained them in foreign languages, the sciences, and area studies.

But by the time the Cold War ended, the intelligence establishment that had served Washington so well in the second half of the twentieth century was sorely in need of change. The post–Cold War "peace dividend" led to a reduction of intelligence staffing by 22 percent

---

Mike McConnell is Director of National Intelligence of the United States.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2007		**00-07-2007 to 00-08-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Overhauling Intelligence (Foreign Affairs, Volume 86, Number 4, July/August 2007)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Director of National Intelligence,Washington,DC,20511**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**10**	

between fiscal years 1989 and 2001. Only now is staffing getting back to pre–Cold War levels. The National Security Act mandated that information be shared up the chain of command but not horizontally with other agencies. At the time of the act's passing, little thought was given to the need for a national-level intelligence apparatus in Washington that could synthesize information from across the government to inform policymakers and help support real-time tactical decisions. That reality, coupled with practices that led to a "stovepiping" of intelligence, arrested the growth of information sharing, collaboration, and integration—patterns that still linger.

All these shortcomings have made the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and the creation of the post of director of national intelligence (DNI) timely and appropriate but, by themselves, insufficient. Indeed, these measures must be only the beginning of a larger reform. The state-sponsored terrorist groups that threaten the United States are accompanied by an ever larger number of nonstate actors moving at increasing speeds across geographic and organizational boundaries. These new actors blur the traditional distinctions between foreign and domestic, intelligence-related and operational, strategic and tactical. To respond, Washington must forge a collaborative approach to intelligence that increases the agility of individual agencies and facilitates the effective coordination and integration of their work.

BRINGING DOWN WALLS

THE POST of DNI was created in 2005 to transform and modernize intelligence institutions, rules, and relationships to meet today's intelligence needs. Since 1947, new threats to U.S. national security have appeared, new missions have been developed, and new intelligence agencies have come into existence. A national intelligence authority was needed to focus, guide, and coordinate all the United States' 16 intelligence agencies to better provide timely, tailored intelligence support to a wide range of users with different, and often competing, requirements. The National Security Act sought to unify U.S. military and foreign intelligence efforts, but it did not envision or provide for today's requirement to integrate intelligence and law enforcement.

Our main challenge in doing this is to strike the right balance between centralized direction and decentralized execution so that the Office of the DNI does not just end up being another layer of bureaucracy on top of the existing structures.

Ensuring the integration of foreign and domestic intelligence collection and analysis, as the 9/11 Commission recommended, is one of the most important responsibilities given to the Office of the DNI—and a vital component of striking that balance. How to do this while respecting and protecting the rights Americans hold dear has been among the most difficult challenges facing the intelligence community. The difficulties have been compounded by the need to operate under the rigid barriers put in place by the National Security Act. Under the act, U.S. intelligence capabilities involve four distinct areas of responsibility: supporting the president, engaging in clandestine activities abroad in support of national policy goals, protecting the United States against Soviet penetration, and supporting strategic military operations. The director of central intelligence and the Central Intelligence Agency (CIA) are given responsibility over the first two, the Federal Bureau of Investigation (FBI) over the third, and military intelligence units over the fourth.

Today, sticking rigidly to these historical distinctions would be a serious impediment to protecting U.S. national security. The United States has enemies who seek to acquire and detonate weapons of mass destruction on U.S. soil. This is a constant and significant threat, and the intelligence community's work to thwart it must not be constrained by policies of the past. U.S. intelligence agencies started to integrate domestic and foreign intelligence operations after the first World Trade Center terrorist attack in 1993 and the follow-on attacks on the Khobar Towers in Saudi Arabia in 1996, the U.S. embassies in East Africa in 1998, and the U.S.S. *Cole* in 2000. The work took on even greater urgency after the tragedy of 9/11. As a result, Americans today benefit from the combined intelligence work of the Department of Homeland Security and the FBI's National Security Branch—an office that brings together the bureau's counterintelligence, counterterrorism, weapons of mass destruction, and intelligence components. The DHS and the FBI are providing a more integrated approach to intelligence in order to protect the United States from foreign and homegrown terrorists.

But even as the wall between domestic and foreign intelligence collection was coming down, a wall between foreign intelligence and law enforcement remained standing. In 1981, for example, the Drug Enforcement Administration was taken out of the intelligence community because of concerns that it would improperly mix intelligence and law enforcement. But that commingling was absolutely necessary: with its large law enforcement presence abroad, the DEA is able to contribute unique narcotics information and overseas experience. Hence, last year, the DNI helped the DEA establish its Office of National Security Intelligence. This newest member of the U.S. intelligence community brings access, insights, and experience in foreign and domestic narcoterrorism.

Coordinating domestic and foreign intelligence continues to be a challenge. The intelligence community has an obligation to better identify and counter threats to Americans while still safeguarding their privacy. But the task is inherently a difficult one. New technology being developed by the Office of the DNI's chief information officer and chief technology officer to access and process vast amounts of digital data to find terrorist-related information is being overseen by the DNI's Privacy and Civil Liberties Office. Another challenge is determining how and when it is appropriate to conduct surveillance of a group of Americans who are, say, influenced by al Qaeda's jihadist philosophy. On one level, they are U.S. citizens engaging in free speech and associating freely with one another. On another, they could be plotting terrorist attacks that could kill hundreds of people.

COME TOGETHER

THE DNI also needs to transform the culture of the intelligence community, which is presently characterized by a professional but narrow focus on individual agency missions. Each of the 16 organizations within the intelligence community has unique mandates and competencies. They also have their own cultures and mythologies, but no one agency can be effective on its own. To capture the benefits of collaboration, a new culture must be created for the entire intelligence community without destroying unique perspectives and capabilities.

The way to do so would be to follow the model provided by the Goldwater-Nichols reforms of the military in the late 1980s. The Goldwater-Nichols Act created a unified military establishment and, among other things, laid the foundations for a "joint" military. It created incentives for interservice collaboration (such as requiring joint service to achieve flag rank) and promoted joint training and development. What Goldwater-Nichols did for the military, IRTPA should provide the means to do for the U.S. intelligence community.

Greater collaboration is vital because no single agency has the capacity to survey all the available information. The U.S. intelligence community collects more than one billion pieces of information every day. Intelligence can only help inform and shape decisions if it is processed through the mind of an analyst who resolves any conflicts and ambiguities. For example, a piece of paper with a list found on a suspected terrorist—known in the field as "pocket litter"—could turn out to be a grocery list or a coded roster of associates. It takes an analyst trained in what to look for to tell the difference. U.S. intelligence agencies will never have enough analysts to fully examine all the data they collect, but the ones they do have can do their job better by developing new ways of thinking about analysis and information distribution in a more integrated community.

As the intelligence community grew during the Cold War, it sometimes acted like anything but a collaborative community. Analysts often did not know their counterparts at other agencies unless they reached out to them on their own. There were few processes in place to collaborate, share lessons learned and best practices, and exchange viewpoints. This approach may have worked during the Cold War, when strategic threats evolved slowly and various streams of analysis could proceed independently before being combined, but it cannot succeed today, when events evolve quickly and require rapid action.

Consider a recent example. In the spring of 2005, the CIA and the military's Northern Command received information about two passengers aboard a plane flying from the Middle East to Mexico that would shortly cross U.S. airspace. Because the flight was not operated by a U.S. carrier and was not scheduled to land in the United States, there was no requirement for the passenger list to be reviewed prior to takeoff. Although the airline's ticket agent thought the two passengers

appeared suspicious, the flight departed before their names could be checked. The airline passed on the names and the flight information to U.S. authorities, however, and this information was funneled to the National Counterterrorism Center, the U.S. government's hub for all counterterrorism intelligence, where analysts can access more than 30 separate government computer networks carrying more than 80 unique data sources. Within hours, the NCTC found information indicating that the two passengers had been placed on a "no-fly list" immediately after 9/11 because they had lived in the United States in the 1990s, had connections to two of the 9/11 hijackers, and possessed pilot's licenses. Based on this information, the plane was denied entry into U.S. airspace, and the pilot decided to return to Europe. The intelligence community's real-time coordination and rapid-response capabilities were essential.

Interagency collaboration needs to be established at two levels: intelligence collection and intelligence analysis. To this end, the Office of the DNI is in the process of developing virtual communities of analysts who can securely exchange ideas and expertise across organizational boundaries and harness cutting-edge technology to find, access, and share information and analytic judgments. Analysts are increasingly using interactive online journals, such as classified blogs and wikis, to this end. Such tools enable experts adept at different disciplines to pool their knowledge, form virtual teams, and quickly make complete intelligence assessments. Interagency joint-duty programs are also being implemented so that personnel from any agency can benefit from the knowledge of the entire intelligence community. An example of progress thus far is the newly created Rapid Analytic Support and Expeditionary Response, or RASER, team, a group of relatively new analysts drawn from all the intelligence agencies who undertake special training so that they can react rapidly to crises, drive intelligence-collection efforts, and work as catalysts for increased integration. Starting this summer, this elite "special forces" analytic team will be ready to be deployed against some of the United States' hardest intelligence targets.

The long-standing policy of allowing officials access to intelligence on a "need to know" basis should be abandoned.

The U.S. intelligence community also needs to know where collection gaps exist, where it needs greater specific intelligence, and on what areas it is overly focused. Some gains have been made with the creation of mission managers—a recommendation of the Weapons of Mass Destruction Commission—who oversee and manage high-interest topics, such as North Korea, Iran, Cuba, and Venezuela, and counterterrorism, counterproliferation, and counterintelligence, for appropriate collection and analysis. The intelligence community is also investing in more in-depth and long-range analysis so that analysts can dig deeper into issues of concern for the future, such as the changing character of warfare and energy security, unencumbered by the demands of producing current intelligence. Furthermore, addressing a critical need emphasized by the 9/11 Commission and the Weapons of Mass Destruction Commission, the intelligence community has formed "devil's advocate" and alternative analyses, examining, for example, whether avian influenza can be weaponized and how webcams could aid in terrorist planning. Beyond these efforts, the intelligence community can still learn a lot from commercial best practices and best-in-class analytic technologies to help its analysts sift through data and more rapidly identify key insights.

CULTURE SHOCK

OLD CULTURES and practices need to be changed so that today's intelligence community can rapidly exchange information between officers on the ground—both at home and abroad—and decision-makers in Washington. Most important, the long-standing policy of only allowing officials access to intelligence on a "need to know" basis should be abandoned. The U.S. intelligence community needs to adopt a mindset guided by a "responsibility to provide" intelligence to policymakers, war fighters, and analysts while still reasonably protecting sources and methods. Significant progress has been made since 9/11, but policy and cultural impediments remain. The challenge now is to convince collectors that they are not data owners so much as data providers.

The way to do so would be to share threat information with state and local officials as well as members of the private sector. The unique contribution made by men and women on the ground is vital to U.S.

national security. In 2000, for example, a county sheriff's investigation into a local cigarette smuggling case in Charlotte, North Carolina, uncovered a multistate terrorist cell supporting Hezbollah. In 2005, a local police detective investigating a gas station robbery in Torrance, California, uncovered a homegrown jihadist cell planning a series of attacks in Illinois. State and local partners should no longer be treated as only first responders; they are also the first lines of prevention. Changing mentalities in this way is the responsibility of the program manager for the Information Sharing Environment, which was created by the IRTPA and exists to foster a partnership between all levels of government and both the private sector and foreign partners in order to share terrorist threat information.

Another important area in which mindsets need to change is in hiring practices. Policy barriers have stood in the way of attracting intelligence professionals with the right skills and backgrounds. The responsibility to protect sources and intelligence-collection methods from unauthorized disclosure has heightened some organizations' risk aversion. As a result, intelligence agencies have faced significant obstacles in hiring some of the people they need most: first- and second-generation Americans with fluency in languages ranging from Albanian to Urdu and with unique political, technical, or scientific skills. These men and women possess cultural insights and skills that no amount of teaching can impart. If the intelligence community is going to reach out to native speakers, it must change its recruitment practices, which currently make it difficult to hire such candidates.

STAYING ON THE CUTTING EDGE

THROUGHOUT THE Cold War, the U.S. intelligence community was at the forefront of technological innovation, be it for weapons systems, computers, or satellite technology. In the last 20 years, its lead has dwindled as innovation has moved from the public to the private sector and technological know-how has spread across the world. Worse still for the United States, its adversaries have been quick to adapt to technological improvements.

The U.S. intelligence community needs to harness the promise of advances in fields such as the biosciences, nanotechnology, and

information technology. The new Intelligence Advanced Research Program Agency seeks to do just that, much as a similar Department of Defense program is doing to drive leading-edge technologies to meet defense requirements. One fruit of that effort was the development in 2004 of Argus—named for the giant from Greek mythology with one hundred eyes—which monitors foreign news media and other open sources for early indications of epidemics or other serious biological incidents, such as increased absenteeism, failures of health-care infrastructure, and other disruptions of normal life. At the outset of the avian flu outbreak in November 2006, Argus became fully operational and provided rigorous, validated information on the disease. Today, it monitors more than one million reports a day from nearly 3,000 sources in 21 major languages in 195 countries. In the future, Argus may be able to use open-source reporting to more rapidly detect other causes of societal disruption—especially in closed societies—such as nuclear accidents and environmental disasters.

Beyond developing technologies, however, it is essential to make sure new tools get from the drawing board to the field. To that end, our Rapid Technology Transition Initiative focuses on invigorating research and development so that ideas can be translated into usable tools quickly and cost effectively. RTTI has already shown its value. Since its deployment late last year, the FBI's Biometric Quick Capture Platform—a portable database funded through RTTI—has facilitated the biometric identification of suspects in custody overseas. It has helped users collect and store fingerprint data and perform real-time electronic searches of federal fingerprint databases. These queries can quickly establish links to a person's previously used identities and past criminal or terrorist record. Just two months after the release of RTTI funds to the FBI, the bureau's field personnel were using this tool to identify whether individuals in custody overseas had criminal records or were dangerous threats to U.S. forces.

But moving cutting-edge technologies into the hands of U.S. intelligence personnel means shortening timelines for developing these technologies. In this area, there is still much work to be done. The U.S. intelligence community's European colleagues, for example, are able to build, launch, and operate a new satellite system in about five years and for less than a billion dollars. By contrast, a U.S. spy satellite

system, although admittedly more complex than a European equivalent, can take more than ten years and cost billions of dollars to develop. This is due, in part, to the larger number of requirements the United States tends to place on individual systems and its higher aversion to the risk of mission failure, both of which increase the systems' complexity and the demands placed on the technology. If the U.S. intelligence community is to close this gap, it will need a more disciplined, agile acquisition policy. It was to this end that the DNI recently elevated the task of acquisitions to the level of a deputy director of national intelligence (there are four deputy directors).

THE END OF THE BEGINNING

ALTHOUGH THE United States is improving the nuts and bolts of its intelligence system, it must not lose sight of the strategic conditions that will determine the ultimate success of those efforts. The United States must comprehend the profound threats of the times and position its institutions to meet those challenges. The intelligence community understands the threats posed by terrorists inside and outside the United States, nuclear proliferators, and rogue and failed states. Now, it must set its priorities to meet these threats.

If the efforts to improve the intelligence community are to endure, they will need sustained support from the executive branch, Congress, and the American people. It will take years to fully clarify and coordinate the DNI's responsibilities and powers, transform the collection and analysis of intelligence, accelerate information sharing, change institutional cultures, build high-tech capabilities, and boost the acquisition of new technologies. And it will take the patience of the American people and their willingness to lend their talent and expertise to the intelligence community.